Claims:

1. (amended) A method of preventing virus infection by detecting the virus infection in a network, comprising steps of:

obtaining communication information when a virus intrudes;

detecting a virus source computer based on the communication information obtained;

sending a message announcing an antivirus attack on the virus source computer; and

making the antivirus attack on the virus source computer.

2. (amended) A method of preventing virus infection according to Claim 1, wherein:

a decoy accessible through the network is provided to a computer that monitors intrusion of a virus, for receiving access to said decoy to obtain communication information and to detect virus intrusion; and

said decoy is one or more of a decoy folder stored in a storage unit, a decoy application stored in the storage unit, and a server formed virtually in the storage unit.

3. A method of preventing virus infection according to Claim 1, wherein:

said attack is made by imposing a high load on the virus source computer.

4. A method of preventing virus infection according to Claim

3, wherein:

said high load is imposed on the virus source computer by increasing traffic of said computer.

5. A method of preventing virus infection according to Claim 3, wherein:

said high load is imposed on the virus source computer by sending a large number of requests to which a CPU of said computer should respond.

6. (amended) A system for preventing virus infection by detecting the virus infection in a network, comprising:

a communication information analysis means that detects intrusion of a virus, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes;

a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus; and

a message sending means that sends a message for announcing a start of the attack, to the infected computer.

7. (amended) A system for preventing virus infection according to Claim 6, wherein:

said system further comprises a decoy means accessible through the network; and

said communication information analysis means detects virus intrusion into said decoy means, and on detection of the

virus intrusion, detects a virus source computer, based on the communication information obtained when the virus intrudes.

8. A system for preventing virus infection according to Claim 6, wherein:

said computer attack means imposes a high load on the virus source computer.

9. (amended) A system for preventing virus infection according to Claim 8, wherein:

said computer attack means imposes the high load on the virus source computer by increasing traffic of said computer.

10. A system for preventing virus infection according to Claim 8, wherein:

said computer attack means imposes the high load on the virus source computer by sending a large number of requests to which a CPU of said computer should respond.

11. (amended) A system for preventing virus infection according to one of Claims 6, 7, 8, 9 and 10, wherein:

said system further comprises a detection report transmission means that sends a detection report to an administrator of the virus source computer; and

said computer attack means continues to make the antivirus attack on the virus source computer until a countermeasure against the virus has been completed.

12. A system for preventing virus infection according to Claim 6, wherein:

said decoy means is a decoy folder realized by an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network.

13. A system for preventing virus infection according to Claim 6, wherein:

said decoy means is a decoy application realized as an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network.

14. (deleted)

15. (amended) A system for preventing virus infection according to one of Claims 6, 7, 8, 9 and 10, further comprising:

an alarm sound generation means that generates an alarm sound in a attacking terminal unit at a start of the attack or after the start of the attack.

16. (amended) A system for preventing virus infection according to one of Claims 6, 7, 8, 9 and 10, further comprising:

a requesting means that notifies a network address of the virus source computer to another computer connected to the network and requests to said computer for making an antivirus attack on the virus source computer.

17. A system for preventing virus infection by detecting the

virus infection in a network, comprising:

a request receiving means that receives a request for making an antivirus attack on a virus source computer; and

a computer attack means that makes an antivirus attack on said virus source computer through the network for suppressing operation of a virus, based on said request received.

18. (amended) A program for making a computer prevent virus infection, wherein:

said program makes said computer realize:

a communication information analysis means that detects intrusion of a virus, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes;

a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus; and

a message sending means that sends a message for announcing a start of the attack, to the infected computer.

19. (deleted)

20. (added) A system for preventing virus infection by detecting the virus infection in a network, comprising:

a communication information analysis means that detects intrusion of a virus, and on detecting virus intrusion, detects a virus source computer, based on communication information obtained when the virus intrudes;

a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus; and

an alarm sound generation means that generates an alarm sound in an attacking terminal unit at a start of the attack or after the start of the attack.

21. (added) A system for preventing virus infection by detecting the virus infection in a network, comprising:

a communication information analysis means that detects intrusion of a virus, and on detecting virus intrusion, detects a virus source computer, based on communication information obtained when the virus intrudes;

a detection report transmission means that sends a detection report to an administrator of the virus source computer.